IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305015 |

Cryptic Passkeys: Passwordless Authentication Using Webauthn

Smiraj K R, Prashant M, Nikhil N, Yogesh, Pratham Majumder

UG Student, Dept. of ISE, Jain (Deemed-to-be) University, Bengaluru, Karnataka, India

Professor, Dept. of ISE, Jain (Deemed-to-be) University, Bengaluru, Karnataka, India

ABSTRACT: A move from password-based authentication to passwordless approaches is being driven by the need for ever-stronger security measures in the digital age. Using the Web Authentication API (WebAuthn) to provide a secure yet easy-to-use authentication process, this paper investigates the use of passkeys. In addition to improving user comfort, this method strengthens security by removing typical password vulnerabilities. Passkeys' technical workings, their incorporation into the systems in place, and their effects on user experience are all assessed in this study.

KEYWORDS: Passkeys, Passwordless Authentication, WebAuthn, Security, User Experience, cryptography.

I.INTRODUCTION

The shortcomings of conventional password-based authentication grow more and more obvious as long as cyber threats persist. Passwords are a major weakness in digital security frameworks since they are frequently readily guessed or stolen. A more secure and convenient solution is promised by the introduction of passwordless authentication technologies, especially those that use cryptographic credentials like passkeys. This paper presents the idea of passkeys, their working mechanism, and their dependence on WebAuthn, a browser-based application programming interface that supports public-key cryptography for user authentication. Our digital lives have become increasingly dependent on passwords; the majority of internet accounts now simply contain a short string of characters that the user knows. According to estimates, the average internet user has more than 100 password-required accounts. Considering that there are billions of internet users globally, this means that trillions of passwords are in use. These widely used codes are necessary for activities like email, banking, and social media use, but they have several well-known flaws that make them extremely vulnerable in terms of security. Prominent data breaches act as painful reminders; in the past year alone, over 1.1 billion passwords at big businesses like Uber, Twitter, and RockYou2021 were leaked, demonstrating how simple it is to steal or hack enormous password databases. A basic problem lies in the way users generate and maintain their passwords: some choose easy solutions based on personal information or dictionary phrases ("123456" or "password"), while others rely on randomly given combinations assigned by the system that are hard to remember. Because of this, people frequently reuse their login credentials for convenience across several platforms, seriously undermining security precautions. Due to these human aspects, it is far too simple for hostile parties to use automated tools and dictionary-based tactics to launch brute force assaults in an attempt to get unauthorized access. Alternatively, much worse, using offline password hashes that have been released to decrypt login credentials by comparing every possible combination with pre-stored algorithms. Thanks to GPU-driven increased processing power, formerly thought-to-be-strong passcodes can now be cracked in hours or minutes as opposed to months in the past.

Alternative authentication methods are required as long as passwords have security and usability issues. Passkeys are a novel approach that seeks to provide secure passwordless authentication for websites and applications. But what are passkeys specifically, and how do they work? In their simplest form, passkeys replace passwords in authentication using public-key cryptography. Instead than entering a plaintext password that needs to be retained and kept safe, passkeys offer secure credential-based authentication associated with a specific device. Passkeys improve both the FIDO (Fast Identity Online) and WebAuthn protocols. Users can create pairs of public and private keys and securely authenticate themselves using biometrics with the use of a web API called WebAuthn. Passkeys exploit this by using asymmetric cryptography.

Since the ubiquitous usage of passwords and their flaws continue to raise security and usability concerns, viable alternatives to password-based authentication are needed. One new technology that seems to have potential is passkeys. With a focus on improved security, privacy, and convenience, passkeys offer passwordless authentication. They use public key cryptography and device-bound credentials to do this. This study argues that passkeys may someday

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305015 |

surpass passwords as the most widely used general-purpose authentication technique for consumers and businesses. Passkey technology still has to be refined, widely used, and its effects and performance in real life evaluated in detail.

II. LITERATURE SURVEY/ EXISTING SYSTEM

The majority of today's authentication methods rely on biometrics, PINs, and passwords. Every approach has its own set of drawbacks and hazards, such as password fatigue and privacy issues with biometric data. The need for solutions that strike a compromise between security and usability is highlighted by recent literature. Research from the FIDO Alliance and other cybersecurity studies highlights the move toward cryptographic techniques. The present section will examine the state of research and many applications of passwordless technology, laying the groundwork for a discussion on passkey integration.

A major change has occurred with the conception and creation of passwordless systems, especially those that make use of cryptographic tokens or devices. Passkeys are at the forefront of this shift, supported by WebAuthn and FIDO2 standards. Passkeys use a type of public key cryptography in which the user must demonstrate that they are in possession of a private key in order to authenticate without actually sending the key (FIDO Alliance, 2021). Using this strategy, a lot of the issues related to 2FA and passwords are effectively eliminated. The creation, management, and application of these cryptographic credentials in user authentication are described in full in a seminal work of literature, the WebAuthn specification published by the World Wide Web Consortium (W3C) and FIDO Alliance (W3C, 2021). It promotes a global standard that guarantees security regardless of the gadget being used.

Subsequent research, such that conducted by Mayer et al. (2022), has concentrated on the adoption rates and user experience of WebAuthn-enabled platforms. According to their research, although there is a learning curve for new authentication techniques, user happiness often rises with increased familiarity because passwordless logins are more convenient and offer superior security. Passkey technology has come a long way, but widespread adoption and cross-platform and cross-device interoperability are still obstacles. Scholars such as Zhang et al. (2023) examine these issues and provide recommendations for how to promote smooth user experiences throughout various technological ecosystems and expedite the adoption process.

The body of research indicates that passkey-based systems are becoming more and more popular as a strong replacement for conventional authentication techniques. As the digital world moves toward more secure and user-friendly authentication processes, more research and development in this field is necessary. Additionally, passkeys increase security by connecting credentials to specific devices through on-device biometric verifications like fingerprint or face recognition. Users have to authenticate to the device before they may use the passkey. By doing this, you can increase security beyond what can be achieved with simple password entering. Passkeys are also impervious to replay attacks. The passkey changes dynamically with each login since it is a signature of a randomly generated challenge nonce. It is not possible to replay static credentials in between sessions. The use of cryptography guarantees that the device containing the associated private key is the only one capable of generating the valid login passkey. By eliminating the requirement for plaintext password transmission and storage, passkeys get around most common password cracking techniques.

Private keys are kept apart on user devices with hardware-backed security measures. It is not feasible to target a central password database. When passkeys are session specific, brute force is not helpful. In conclusion, security features provided by passkey technology are fundamentally better than those of password-based authentication. Passkeys solve a lot of the problems related to employing static password secrets in different circumstances. To improve end-user security without compromising usability, biometric binding, hardware-secured private keys, and cryptographically signed responses all function effectively. As their use grows, passkeys are well-positioned to usher in a new era of passwordless authentication.

III. PROPOSED METHODOLOGY AND DISCUSSION

Public-key cryptography is used by passkeys to enable passwordless authentication. This is not the same as conventional password authentication, which is based on secret keys that are shared. Using key pairings made up of a public key and a private key, public-key cryptography improves security. The user provides their password text, which serves as a shared secret key, in order to enable password authentication. During each login session, the same static password is used for authentication. Every time, the system hashes the password and compares it to the hash that is kept in order to verify. But because the secret is routinely communicated and kept, this arrangement leaves passwords open

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305015 |

to interception or leakage. This problem is resolved by public-key cryptography, which uses asymmetric key pairs rather than shared secrets. The client device uses the WebAuthn API to create a distinct public/private key pair during passkey enrolment. While the public key is transferred and stored on the server, the private key is kept safe on the client device. Never let the private key escape the device. The server sends the client a challenge nonce for login. Next, using their private key, the client signs this nonce locally and returns the signature to the server. The passkey, a transient credential specific to that session, is this signature. By comparing the signature to the public key it has on file for that user account, the server verifies the passkey.

Hardware security mechanisms such as Trusted Platform Modules (TPM) and Secure Enclaves are leveraged by the private keys used in passkey generation. This provides security by isolating them from other processes and operating systems. When private keys are not actively signing authentication challenges, they are encrypted. A second factor is provided by biometric checks, such as fingerprint or face recognition, which demand user authentication prior to the private key being able to sign anything. The hardware and the authorized user are both tied to the keys. To authenticate against the public key record, a signature can only be produced using the private key. The public keys themselves are not private and can be securely kept on servers or in databases. Never is a shared password sent over the air or kept in plain sight. Because the keys are asymmetric, passkeys are also immune to man-in-the-middle and phishing assaults. The public key cannot be used to generate or reconstruct the private key. Without the corresponding private key, intercepting the public key or signatures is insufficient for authentication. By utilizing strong public key cryptography, which is already widely used in fields like TLS certificates and end-to-end encrypted transmission, passkeys improve security. Unlike conventional password techniques, passkeys allow passwordless login without ever disclosing or transmitting the secret signature key when used for authentication. Every login challenge response is distinct and verifiable cryptographically via the validation of public and private keys.

Passkeys readily connect into a variety of applications and websites by utilizing industry-standard cryptographic protocols and API specifications. Among these essential elements are the FIDO standards and the Web Authentication API (WebAuthn), which enable passwordless authentication. A browser-based interface for managing public key credentials linked to passkeys is made possible by the WebAuthn component. The novel "create()" function safely stores the private key on the client's device and creates a distinct public/private key pair during registration. After that, the matching public key is sent to the server. Users can use WebAuthn's "get()" function for authentication purposes to verify signatures. This is done by using their private keys and personalized challenge nonce to create a secure passkey signature, which is then returned to verify authenticity. Developers are relieved of the burden of handling intricate cryptographic processing and storage issues thanks to this simplified procedure. Furthermore, FIDO protocols that are specifically created to improve web-based user validation procedures through additional standardization efforts are building upon these advancements. Specifically, these protocols are used within servers themselves, utilizing their Relying Party feature as a crucial means of authenticating requests for both registration and authentication, which are made possible by specialized clients known as "FIDO Authenticators."

Essentially, during the registration phase, this proprietary model makes use of extensive data parameters provided by Receiving Parties to generate unique challenges, such as matching metadata arrays linked to the creation of appropriate Public/Private Key pairs, thanks to advanced response objects. These objects accompany our customized user IDs, which include credentials neatly embedded inside said forms, and finally allow Server Validation to check the appropriate boxes for complete online enrollment." In order to make our ground-breaking method even more alluring than it was previously, the second phase entails creating extremely detailed instructions about three crucial elements that are inherent here 1). First up? Registration! Just sit back and relax now guys because we have you covered completely one hundred per cent reliably no matter what happens every single time without fail it shows! 2). Next comes the challenging part– Authentication itself indeed includes issuing customized requests for respective nonces-then further enhancing them to provide completely satisfactory verification services throughout this entire process-matching Public Keys and Parameters flawlessly all while verifying the authenticity of the user's identity overall; not only is it highly convenient but also delivers unparalleled security levels as well! 3). In order to improve matters even further, we have gone above and beyond with our incredible FIDO-certified solutions, making it possible for more simple integration options to be made available on websites and applications without requiring any extra work from you guys. As a result, no matter where your business needs us most, you can always count on us to be there—WebAuthn API! PIs are in charge of lower-level cryptography and key elements management. The two primary methods of FIDO authentication are second factor and passwordless. In the former scenario, passkeys are used as the only credential, negating the need for a backup password; in the later scenario, additional protection is provided by requiring both password and passkey verification.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305015 |

Prominent companies like Apple, Google, and Microsoft have started integrating passkey functionality natively into their client-side hardware and operating systems. This will make it possible for passkeys to be used seamlessly across FIDO-compliant apps and websites. Furthermore, WebAuthn removes the need for any plugins or proprietary apps. When it comes to deployment, it could be essential to integrate with current account systems in order to support registration procedures that adhere to FIDO protocols. Additionally, in order to validate responses from WebAuthn requests during login processes, Relying Party servers need to be set up properly.

Identity providers have the potential to accelerate the adoption of FIDO technology by providing pre-made solutions. This is where they may play a crucial role. Over time, there has been a significant decrease in the dependence on technical details regarding pass key adoption in native mobile applications and browser-based platforms. This is due to the development of standardized protocols such as WebAuthn and the essential specifications they provide. This suggests a future where passwords may be eliminated in favor of turnkey services provided by platform-specific support.

IV. RESULT AND DISCUSSION

Figure 1 displays the application's webpage, where you can register a new passkey or log in using your existing one.

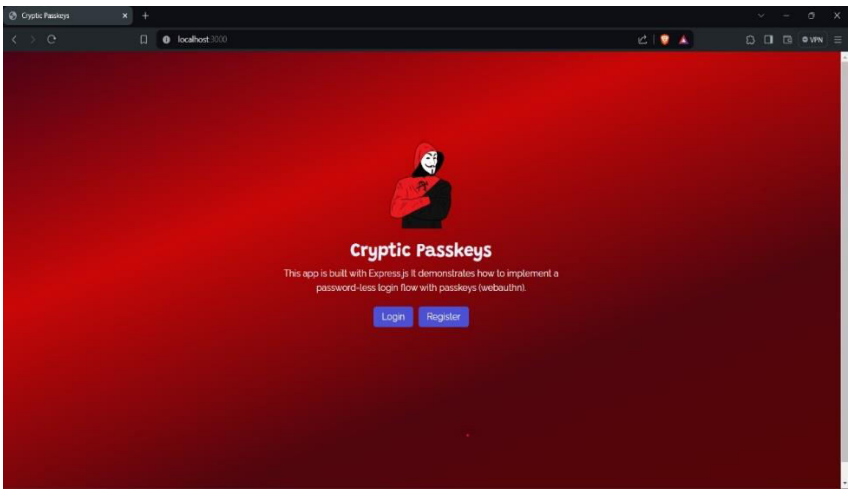

Fig. 1. Webpage used to login or register.

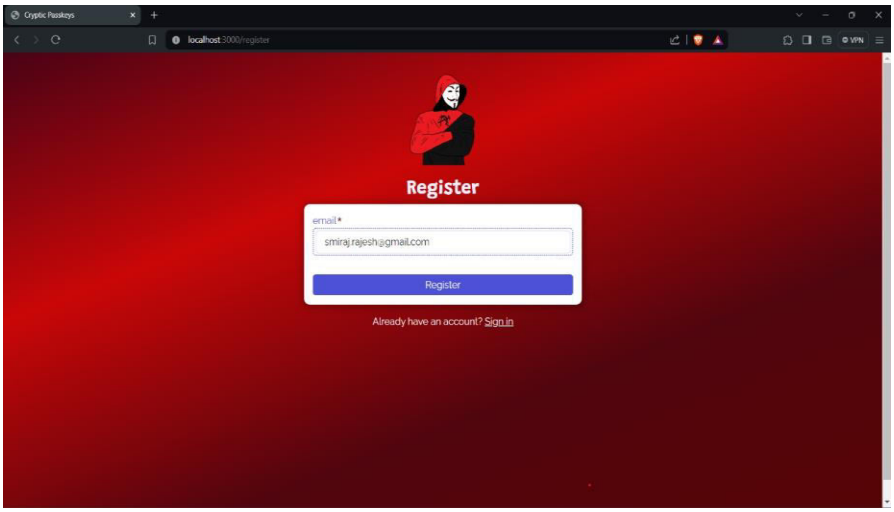

Fig. 2. Registering with e-mail

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305015 |

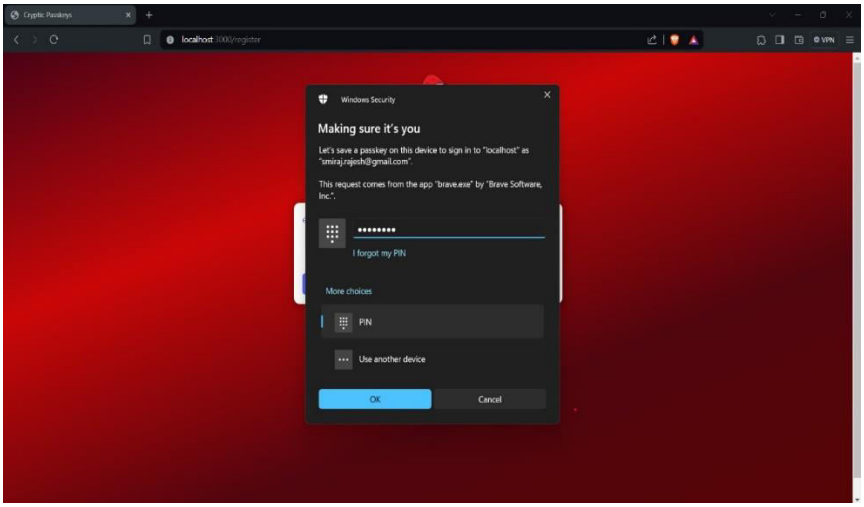

Fig. 3. Authenticator as local computer.

The steps to register a new passkey in Figures 2 and 3 call for the provision of an email address for identification purposes and the usage of an authenticator (such as a computer, smartphone, or other device) to store the passkey and verify the user.

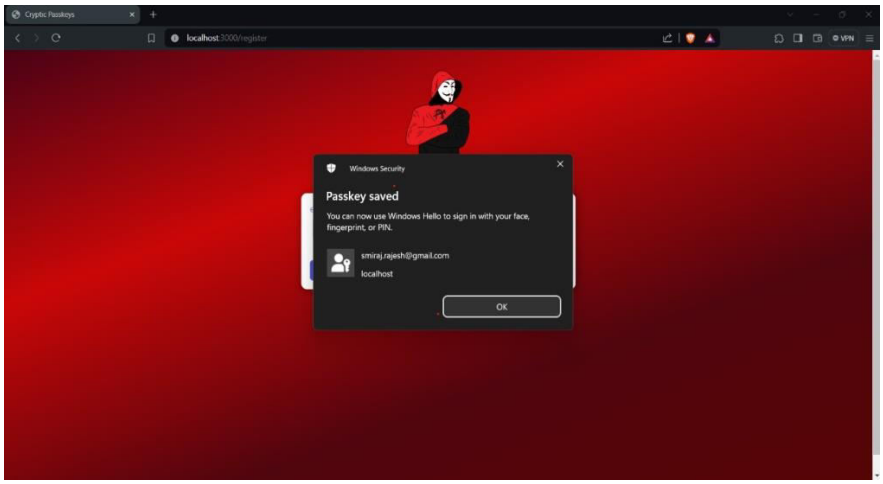

Fig. 4. Passkey saved in the system.

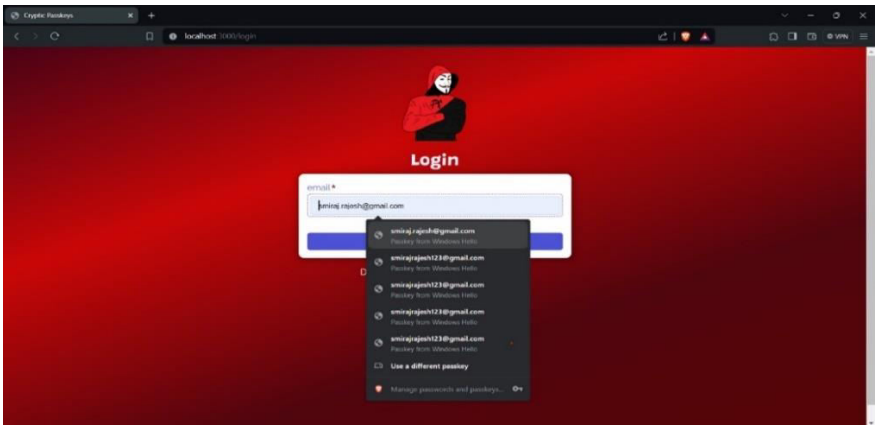

Fig. 5. Loging with the same account.

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305015 |

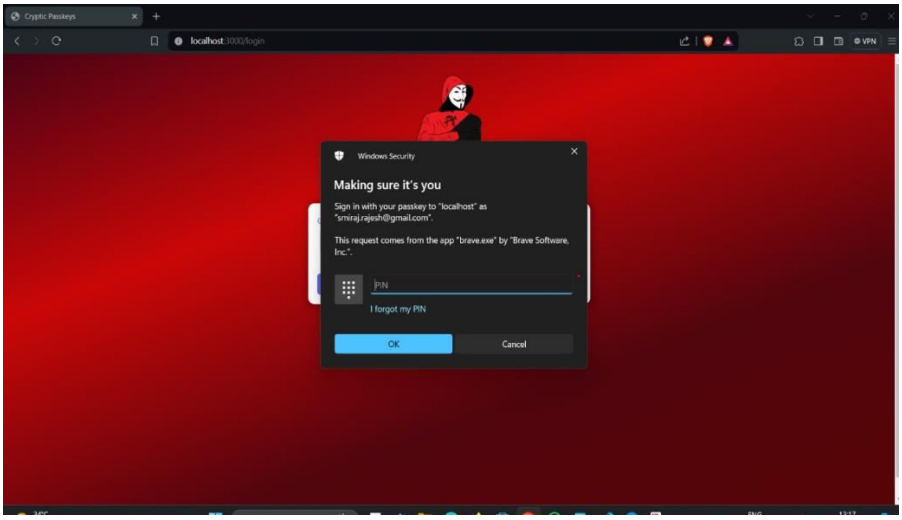

Fig. 6. Entering authenticator password.

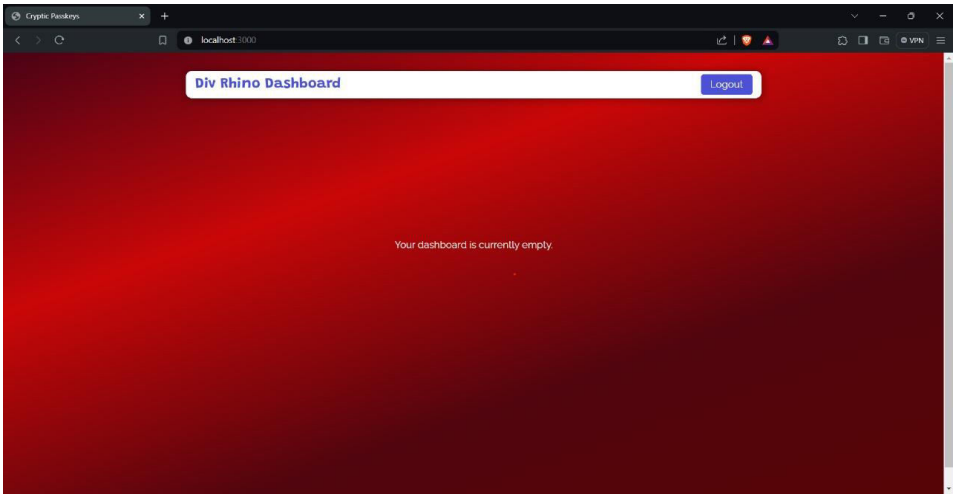

Fig. 7. Dashboard after login.

Following the passkey saving process depicted in Figure 4, we will attempt to log in or authenticate using the same user ID as displayed in Figures 5 and 6.

V.CONCLUSION

By storing private keys on devices rather than in susceptible databases, passkeys, which make use of device-bound credentials and public key cryptography, provide a safe and convenient substitute for traditional passwords. They also increase resilience to phishing and other frequent attacks. Though they have advantages, widespread adoption is hindered by things like user retraining, system upgrades, and deeply ingrained password habits. Platform providers are constantly working to enhance cross-device syncing and secure device roaming, which are still essential for ease. Wider adoption is further hampered by consumer mistrust and the perception of passkeys' utility in comparison to well-known passwords. While passkeys have several drawbacks, such as device dependence, their potential to revolutionize online authentication may cause their adoption to happen gradually but steadily if these issues are resolved by continued design and technology advancements.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305015 |

REFERENCES

[1] P. (2023, November 7). Support for passkeys in Windows - Windows Security. Support for Passkeys in Windows - Windows Security | Microsoft Learn. https://learn.microsoft.com/en-us/windows/security/identity-protection/passkeys/

[2] Wash, R., & Rader, E. (2021, January 1). Prioritizing security over usability: Strategies for how people choose passwords. OUP Academic. https://doi.org/10.1093/cybsec/tyab012.

[3] Shaji George, D. A., & Hovan George, A. S. (2023, December 11). The Emergence of Cybersecurity Medicine: Protecting Implanted Devices from Cyber Threats | Partners Universal Innovative Research Publication. The Emergence of Cybersecurity Medicine: Protecting Implanted Devices From Cyber Threats | Partners Universal Innovative Research Publication. https://doi.org/10.5281/zenodo.10206563R. Chen et al., "Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks," IEEE Commun. Mag., vol. 46, pp. 50–55, Apr. 2008.

[4] Hyder, M. A., & Razzak, J. (2020, November 24). Telemedicine in the United States: An Introduction for Students and Residents. PubMed Central (PMC). https://doi.org/10.2196/20839Y.-C. Liang et al., "Sensing-Throughput Trade-off for Cognitive Radio Networks, "IEEE Trans. Wireless Commun., vol. 7, pp. 1326–37 ,April 2008.

[5] Passkey Authentication: Passwordless entry into online accounts. (2023, July 17). Passkey Authentication: Passwordless Entry Into Online Accounts. https://www.iplocation.net/passkey-authentication-passwordless-entry-into-online-accountsK. M. Passino, "Biomimicry of bacterial foraging for distributed optimization," IEEE Control Systems Magazine, vol. 22, no. 3, pp. 52-67, 2002.

[6] Guide to Web Authentication. (n.d.). Guide to Web Authentication. https://webauthn.guide.

[7] Trevino, A. (2023, October 17). Passkey vs Password: What's the Difference? Keeper Security Blog - Cybersecurity News & Product Updates. https://www.keepersecurity.com/blog/2023/10/17/passkey-vs-password-whats-the-difference/H. Khalife, N. Malouch, S. Fdida, "Multihop cognitive radio networks: to route or not to route," IEEE Network, vol. 23, no. 4, pp. 20-25, 2009.

[8] Passkey Authentication: Google's Passwordless Breakthrough. (2023, June 6). Exabytes (Singapore) Official Blog. https://www.exabytes.sg/blog/passwordless-with-passkeys-authentication/P. K. Visscher, "How Self-Organization Evolves," Nature, vol. 421, pp. 799–800 Feb.2003.

[9] Shaji George, D. A. Securing the Future of Finance: How AI, Blockchain, and Machine Learning Safeguard Emerging Neobank Technology Against Evolving Cyber Threats | Partners Universal Innovative Research Publication. Securing the Future of Finance: How AI, Blockchain, and Machine Learning Safeguard Emerging Neobank Technology Against Evolving Cyber Threats | Partners Universal Innovative Research Publication. https://doi.org/10.5281/zenodo.10001735

[10] G. (2023, May 5). Making authentication faster than ever: passkeys vs. passwords. Google Online Security Blog. https://security.googleblog.com/2023/05/making-authentication-faster-than-ever.html

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details